

AMENDMENTS

In the Drawings:

Replace the original drawing sheets with the attached drawing sheets.

Figure 5 has been amended to correctly identify the “Transaction Coordinator” using reference numeral 202 rather than 310.

Figure 6 has been amended to add reference numeral 222 which identifies the “Bank Interface.”

Figures 6 and 11 have been amended to correctly identify the “TBV Data” using reference numeral 232 rather than 252.

REMARKS

Claims 1-86 are pending and stand rejected. Claims 18, 35, 50 and 68 have been amended.

The Examiner objected to the first line of the abstract as failing to comply with 37 CFR 1.72(b) as detailed in MPEP 608.01(b). Applicants have amended the abstract such that it is now in compliance with the Examiner's recommendations.

Applicants have also amended the specification such that the trademarked terms "Netscape Communicator" and "Microsoft" are capitalized as per the Examiner's suggestion.

The Examiner objected to Figure 1, asserting that the reference characters 102, 104 and 201 have been used to identify the participant. In accordance with the telephonic interview between the Examiner and applicants' representative, Adam Keser, conducted on March 9, 2005, applicants respectfully submit that the drawings are in compliance with 37 CFR 1.84(p)(4). As conceded by the Examiner, the specification, particularly pages 3-5, adequately describes the reference numerals in relation to the entities they represent. Therefore, these remarks are responsive to the Examiner's objection, and the Figures are not amended in response to this objection.

Applicants have amended Figure 5 to correctly identify the "Transaction Coordinator" using reference numeral 202 rather than 310.

Applicants have amended Figure 6 to add reference numeral 222 which identifies the "Bank Interface."

Applicants have amended Figures 6 and 11 to correctly identify the "TBV Data" using reference numeral 232 rather than 252.

Claims 18, 35, 50 and 68 stand rejected under 35 USC 101 for failing to claim statutory subject matter. Applicants have amended claims 18, 35, 50 and 68 to recite statutory subject matter, thereby overcoming this rejection.

Claims 1-17 stand rejected under 35 USC 102(e) over Orrin (U.S. Patent Publication No. 202/0128940). Applicants traverse this rejection.

Claim 1 recites a method of verifying the trustworthiness of a browser comprising creating a first signature, wherein the first signature has as an attribute a “second digital signature verifying the authenticity of one or more components running in an environment of the browser on [a] second computer.” Orrin fails to disclose or suggest such a feature.

Pages 3-4, paragraphs 0038-0043, of Orrin, as cited by the Examiner, instead disclose only the method shown in Orrin’s Figure 2b. In the disclosed method, an Obligor/Borrower 102 digitally signs a document and then verifies himself to a trusted server 100. The Obligor/Borrower then transfers the signed document 210 to an Obligee/Lender 104 who in turn digitally signs the document. The signed document 210 is then transferred along with both digital signatures to the trusted server 100 which validates both signatures and signs an electronic record 200 with its own signature.

None of the above signatures comprise a “second digital signature verifying the authenticity of one or more components running in an environment of the browser on [a] second computer” as recited in claim 1. Furthermore, Orrin does not disclose or suggest verifying the authenticity of any browser components, and thus does not disclose or suggest all of the features recited in claim 1. Therefore claim 1 is allowable over Orrin.

Claims 2-17 depend from allowable claim 1 and are therefore also allowable.

Claims 18-49 stand rejected under 35 USC 102(e) over Shear (U.S. Patent No. 6,292,569). Applicants traverse this rejection.

Claim 18 is directed at creating a “known-good,” or trusted, first set of hashes related to a browser, wherein the first set of hashes comprises a plurality of hashes that correspond to components of a browser. A second set of hashes related to a browser of unknown trustworthiness are then created at a second point in time. The second set of hashes are then compared to the first set of “known-good” hashes to determine the trustworthiness of the browser which was running on a computer at the second point in time. As described in the specification, a major benefit of the

recited method is that content sent from the browser can accepted as trustworthy if the browser that signs or sends the content is verified as trustworthy.

The method recited in claim 18 differs from that disclosed by Shear. Shear discloses (see FIG. 5; col. 10, line 55, through col. 11, line 21; col. 12, lines 16-55; abstract) a method to verify the trustworthiness of "load modules" which are transmitted from one computer to another computer using hash functions. In Shear, a when a load module is to be transferred from one computer to another, the load module is first verified by a verifying authority. When the verifying authority is satisfied with the trustworthiness of the load module, the load module is digitally signed. The digitally signed load module is then subject to a hash function to create a unique message digest. The message digest is then encrypted using a private key. This encrypted message digest is then transferred along with a digitally signed load module to a second computer. The second computer then subjects the transferred load module to the same hash function used by the first computer, thereby generating a second message digest. The two message digests are then compared, and if they do not match, the incoming load module is considered faulty.

Shear discloses verifying the trustworthiness of a load module and signature which are transferred from one computer to another, whereas the method of claim 18 verifies a digital signal by verifying the trustworthiness of the browser that generates the digital signature.

Shear does not disclose or suggest verifying the trustworthiness of a browser as recited in claim 18. Claim 18 is therefore allowable.

Claim 35 also recites verifying the trustworthiness of a browser and is therefore also allowable over Shear.

Claims 19-34 and 36-49 depend from allowable claims 18 and 35 and are therefore also allowable.

Claims 50-86 stand rejected under 35 USC 103(a) over Shear. Applicants traverse this rejection.


Independent claims 50 and 68 both recite verifying the trustworthiness of a browser and are therefore allowable, along with dependent claims 51-67 and 69-86, over Shear for at least the same reasons detailed above regarding claim 18.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. Accordingly, the Examiner is respectfully requested to withdraw the outstanding rejection of the claims and to pass this application to issue. If it is determined that a telephone conference would expedite the prosecution of this application, the Examiner is invited to telephone the undersigned at the number given below.

In the event the U.S. Patent and Trademark office determines that an extension and/or other relief is required, applicants petition for any required relief, including extensions of time, and authorize the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 03-1952 referencing docket no.3880220018. However, the Commissioner is not authorized to charge the cost of the issue fee to the Deposit Account.

Dated: March 15, 2005

Respectfully submitted,

By 
Adam Keser
Registration No. 54,217
MORRISON & FOERSTER LLP
1650 Tysons Blvd, Suite 300
McLean, Virginia 22102
(703) 760-7301